



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/406,910	09/24/1999	DAVID SCOTT HAYES	RIC-98-054	2067
25537	7590	09/09/2004	EXAMINER	
			ZIA, SYED	
		ART UNIT		PAPER NUMBER
		2131		
DATE MAILED: 09/09/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/406,910	HAYES, DAVID SCOTT	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 13 August 2004.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-17 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 13, 2004 has been entered.

Response to Amendment

This office action is in response to arguments filed on June 08, 2004. Original application contained Claims 1-16. Applicant previously added new Claim 17. Applicant amended Claims 1, 4, and 14-17. The amendment filed on June 08, 2004 have been entered and made of record. Presently pending claims are 1-17.

Response to Arguments

Applicant's arguments filed on August 13, 2004 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1 applicants argued that the cited prior art (CPA) [Matyas et al. U.S. Patent No. 5,200,999] at least does not teach, " *a first digital signature of the first public key based on a private key from the certificate authority, and a second digital signature of the second public key base don the first private key* " and also does not disclose that " *PR2 master is not kept outside the cryptographic facility, and PR2 master key is shorter than itself* ".

This is not found persuasive. As discussed in previous office action that CPA teaches a method of managing public key cryptographic system in data processing system using as system master key private and public key pair of commutative asymmetric cryptographic algorithm that includes two pairs, each containing a public key and a private key in the data processing system, for use with respective public key algorithm. A private control vector is then assigned for the private keys for defining permitted uses for the two keys. A private key record is formed which includes the both second private keys, and the private key record is encrypted under a first master key expression which is a function of the private control vector. A private key token is formed which includes the private control vector and the private key record, and the private key token is stored in the data processing system.

Thus, the system provides a method allowing new and expanded key usage to be added to architecture, and single consistent method for handling both public and private keys. Users can port their public and private keys from one cryptographic system to another.

As a result, C PA does implement and teaches a system and method of data authentication utilizing a combination of public key cryptography and digital signatures

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

Art Unit: 2131

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that CPA does teach or suggest the subject matter broadly recited in independent Claims 1, 13-17 and in subsequent dependent Claims 2-12. Accordingly, rejections for claims 1-17 are respectfully maintained.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

a person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Matyas et al. (U.S. Patent 5,200,999).

3. Regarding claim 1 Matyas teaches and describes a method for authenticating transmitted data in real time, the method comprising the steps of:

- generating a master cryptographic key pair, including a first public key and a first private key, publishing a first certificate issued by a certificate authority, the first certificate including the first public key and a first digital signature of the first public key based on a private key from the certificate authority, generating a disposable cryptographic key pair, including a second public key and second private key, generating a second certificate, the second certificate including the second public key and a second digital signature of the second public key based on the first private key (col.12 line 28 to col.13 line 9, col.68 line 15 to line 55, and col.129 line 4 to line 14);

- publishing the second certificate, signing data to be transmitted with a third digital signature by processing the data to be transmitted through a first one way hashing function to generate a first hash value and encrypting the first hash value utilizing the second private key, processing received data through the first one way hashing function to create a second hash value, decrypting the received third digital signature utilizing the second public key to obtain a third hash value, and verifying authenticity of the data by comparing the second hash value to the third hash value (col.24 line 43 to col.26 line 14).

4. Regarding claim 13 Matyas teaches and describes a method for digitally signing data in real time, the method comprising the steps of:

- generating a master key pair including a first public key and a first private key, publishing a first certificate, the first certificate including the first public key and

a first digital signature based on a key pair of a certificate authority', generating a disposable key pair, the disposable key pair including a second public key and a second private key, and wherein the disposable key pair is shorter than the master key pair, generating a second certificate, the second certificate including the second public key and a second digital signature based on the master key pair (col.12 line 28 to col.13line 9);

- dividing the data to be signed into packets, for each packet of data, computing a hash value based on the data in that data packet utilizing a one way hashing function, encrypting the hash value utilizing the second private key as the encryption key, and coupling each encrypted hash value with its corresponding data packet (col.24 line 43 to col.26 line 14).

5. Regarding claim 14 Matyas teaches and describes a method for verifying digitally signed data in real time, the method comprising the steps of:

- processing a data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each packet of digitally signed data, verifying a contents of a first certificate issued by a certificate authority utilizing a public key issued by the certificate authority, the first certificate including a first public key of along master key pair (col.24 line 43 to col.26 line 14);

- verifying a contents of a second certificate issued by a sender of the data utilizing the first public key from the first certificate, the second certificate including a second public key of a short disposable key pair that is shorter than the long master key pair, decrypting a digital signature portion of the digitally signed data utilizing the second public key to obtain a

Art Unit: 2131

second hash value; and comparing the first and second hash values (col.19 line 58 to col.21 line 45).

6. Regarding claim 15 Matyas teaches and describes a method for digitally signing data in real time, the method comprising the steps of:

- generating a disposable key pair, the disposable key pair including a short public key and a short private key, publishing the short public key and a digital signature of the public key based on a long private key longer than the short private key, dividing data to be signed into packets, for each packet of data, computing a hash value based on the data in the data packet utilizing a one way hashing function, encrypting the hash value utilizing the short private key, and coupling each encrypted hash value with its corresponding data packet (col.7 line 18 to col.8 line 15, and col.19 line 58 to col.21 line 45).

7. Regarding claim 16 Matyas teaches and describes a method for verifying digitally signed data in real time, the method comprising the steps of:

- processing a data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each packet of digitally signed data, decrypting a digital signature portion of the digitally signed data utilizing a published short public key to obtain a second hash value, and comparing the first and second hash values, and verifying a digital signature of the short public key based on a long public key, wherein the short public key is shorter than the long public key (col.6 line 4 to line 14, and col.24 line 43 to col.26 line 14).

Art Unit: 2131

8. Regarding claim 17 Matyas teaches and describes a method for verifying digitally signed data in real time, the method comprising the steps of:

- receiving a data packet including an unencrypted data portion and a digital signature portion, generating a first hash value by processing the received unencrypted data portion through a one way hashing function, and decrypting the received digital signature utilizing a public key to obtain a second hash value; verifying the digitally signed data by comparing the first hash value to the second hash value, and verifying the public key based on a digital signature of the public key issued by a certificate authority (col.6 line 4 to line 14, and col.24 line 43 to col.26 line 14).

9. Claims 2-12 are rejected applied as above in rejecting claim 1. Furthermore, Matyas teaches an authentication the method for authenticating transmitted data in real time wherein –

- the step of generating a master key pair comprises creating long first public and private keys (col.7 line 18 to col.8 line 15);

- the first certificate further includes an identification of a sender and an identification of a certificate authority issuing the first certificate (col.2 line 47 to col.3 line 30);

- the first digital signature is produced by processing information representing the identification of the sender, the identification of the certificate authority issuing the first certificate and the first public key through a second one way hashing function to create a fourth hash value; and encrypting the fourth hash value utilizing the private key from the certificate authority issuing the first certificate to create the first digital signature (col.19 line 59 to col.21 line 45);

Art Unit: 2131

- the step of verifying authenticity of data comprising the first certificate (col.10 line 11 to line 32);
 - the step of verifying the authenticity of the data comprising the first certificate comprises: decrypting the first digital signature to obtain a fifth hash value utilizing a public key issued by the certificate authority issuing first certificate, processing the received information representing the identification of the sender, the identification of the certificate authority issuing the first certificate and the first public key through the second one way hashing function to create a sixth hash value; and comparing the fifth and sixth hash values (col.19 line 58 to col.21 line 45);
 - the step of generating a disposable cryptographic key pair comprises generating short second public and private keys (col.7 line 18 to col.8 line 15);
 - the second certificate further includes the identification of the sender and an identification of a signing authority issuing the second certificate (col.2 line 47 to col.3 line 30);
 - the second digital signature is produced by processing the data representing the identification of the sender, the identification of the signing authority issuing the second certificate and the second public key through a one way hashing function to create a seventh hash value; and encrypting the seventh hash value utilizing the first private key to create the second digital signature (col.19 line 59 to col.21 line 45);
 - the step of verifying the authenticity of the data comprising the second certificate (col.10 line 11 to line 32);
 - the step of verifying the authenticity of the data comprising the second certificate comprises decrypting the second digital signature to obtain an eighth hash value utilizing

Art Unit: 2131

the first public key, processing the received data representing the identification of the sender, the identification of the signing authority issuing the second certificate and the second public key through the third one way hashing function to create a ninth hash value; and comparing the eighth and ninth hash values (col.19 line 58 to col.21 line 45);

- dividing the data into packets and signing and authenticating each packet of data in accordance with steps (f) through (i) of claim 1 (col.9 line 35 to line 54).

Art Unit: 2131

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 703-305-3881. The examiner can normally be reached on Monday - Friday 9:00 AM to 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


sz
September 1, 2004